APIs are a centerpiece of digital life. APIs are an efficient and developer-friendly means to unlock value, enabling interoperability of software and data assets with flexibility, speed, and portability. Many digital transformation initiatives are accelerating API adoption, including:

- Public cloud services
- Microservices application design
- Open banking
- Mobile healthcare
- New business and developer ecosystems
- Back office digitization
- Growth trajectory - GraphQL, gRPC, webhooks

As enterprises build their business upon APIs, they have experienced a significant increase in API security incidents. According to Gartner, APIs will be the top attack vector for web applications by 2022, and according to IBM, two thirds of cloud breaches are tied to API misconfigurations.

Noname Security protects APIs in real-time and detects vulnerabilities and misconfigurations before they are exploited. The Noname API Security Platform is an out-of-band solution that integrates with your API gateways, load balancers, and WAFs to offer deeper visibility and security.

**Digital Transformation Requires API Transformation**

**API Security Posture**

- Inventory every API, including legacy and shadow APIs, with data classification.
- Identify misconfigurations and vulnerabilities in source code, network configuration, and policy.

**API Runtime Security**

- Behavioral-based models for runtime API threat detection.
- Automated and semi-automated blocking and remediation of threats.

**Secure API Code**

- Continuously test APIs to identify API risks before they emerge.
- Automated and dynamic test development and incorporation into CI/CD pipelines.
Industry-Leading Approach to API Security

Discover All APIs, Data, and Metadata
Find and inventory every kind of API, including HTTP, RESTful, GraphQL, SOAP, XML-RPC, and gRPC. Discover legacy and rogue APIs not managed by an API gateway, and catalogue API attributes and metadata.

Analyze API Behavior and Detect API Threats
Use automated AI-based detection to identify the broadest set of API vulnerabilities, including data leakage, data tampering, misconfigurations, data policy violations, suspicious behavior, and attacks.

Prevent Attacks, Remediate API Vulnerabilities
Prevent attacks in real-time, fix misconfigurations, automatically update firewall rules, webhook into your WAFs to create new policies against suspicious behavior, and integrate with existing workflows (including ticketing and SIEMs).

Actively Test APIs Before Production
Most applications are tested before they are deployed into production. Most APIs are not. Actively test APIs as part of the software development lifecycle to identify issues before production.

About Noname Security
Noname Security is the only company taking a complete, proactive approach to API Security. Noname works with 20% of the Fortune 500 and covers the entire API security scope across three pillars — Posture Management, Runtime Security, and Secure API SDLC. Noname Security is privately held, remote first with headquarters in Palo Alto, California, and an office in Tel Aviv and Amsterdam.

Nonamesecurity.com | info@nonamesecurity.com | +1 (415) 993-7371